**Vendor:**Microsoft

**Exam Code:**98-367

**Exam Name:**Security Fundamentals

**Version:**Demo

**QUESTION 1**

You suspect a user\\'s computer is infected by a virus. What should you do first?

A. Restart the computer in safe mode

B. Replace the computer\\'s hard disk drive

C. Disconnect the computer from the network

D. Install antivirus software on the computer

Correct Answer: D

---

**QUESTION 2**

Physically securing servers prevents:

A. Theft

B. Compromise of the certificate chain

C. Man-in-the middle attacks

D. Denial of Service attacks

Correct Answer: A

---

**QUESTION 3**

Which of the following can be installed and configured to prevent suspicious emails from entering the user\\'s network?

A. Kerberos

B. Single sign-on (SSO)

C. TCP/IP protocol

D. Microsoft Forefront and Threat Management Gateway

Correct Answer: D

To prevent suspicious emails from entering the network, it is required to install Microsoft Forefront and Threat Management Gateway and configure it so that it can block any malicious emails. Exchange server has many spam filtering tools

but Forefront and TMG are additional security measures used for enhancing the protection of the system.

Answer: B is incorrect. Single sign-on (SSO) is defined as a mechanism in which a single action of user authentication and authorization is used to allow a user to access all computers and systems where he got a access permission, without entering passwords for multiple times.

Answer: A is incorrect. Kerberos is defined as a secure method used for authenticating a request for a service in a computer network. Answer: C is incorrect. TCP/IP protocol is used to define the rule computers are required to follow for

communicating with each other over the internet.

---

**QUESTION 4**

Which of the following is the process used by attackers for listening to the network traffic?

A. Eavesdropping

B. Subnetting

C. Sanitization

D. Hacking

Correct Answer: A

Eavesdropping is the process of listening to private conversations. It also includes attackers listening the network traffic. For example, it can be done over telephone lines (wiretapping), email, instant messaging, and any other method of

communication considered private.

Answer: C is incorrect. Sanitization is the process of removing sensitive information from a document or other medium so that it may be distributed to a broader audience. When dealing with classified information, sanitization attempts to

reduce the document\\'s classification level, possibly yielding an unclassified document. Originally, the term sanitization was applied to printed documents; it has since been extended to apply to computer media and the problem of data

remanence as well.

Answer: D is incorrect. Hacking is a process by which a person acquires illegal access to a computer or network through a security break or by implanting a virus on the computer or network.

Answer: B is incorrect. Subnetting is a process through which an IP address network is divided into smaller networks. It is a hierarchical partitioning of the network address space of an organization into several subnets. Subnetting creates

smaller broadcast domains. It helps in the better utilization of the bits in the Host ID.

---

**QUESTION 5**

Which of the following is a tool that can be used to evaluate the servers having vulnerabilities that are related to the operating system and installed software?

A. DNS dynamic update

B. Windows Software Update Services

C. Read-Only domain controller (RODC)

D. Microsoft Baseline Security Analyzer

Correct Answer: D

Microsoft Baseline Security Analyzer is a tool that can be used to evaluate the servers having vulnerabilities that are related to the operating system and installed software Microsoft Baseline Security Analyzer (MBSA) is a software tool of

Microsoft to determine security state by assessing missing security updates and less- secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server,

and Microsoft Office macro settings. Microsoft Baseline Security Analyzer (MBSA) includes a graphical and command line interface that can perform local or remote scans of Windows systems.

Answer: B is incorrect. Windows Server Update Services (WSUS) is an add- on component of Windows Server 2008. It provides functionality to a server to run as a Windows Update server in a Windows network environment. Administrators

can configure a WSUS server as the only server to download updates from Windows site, and configure other computers on the network to use the server as the source of update files. This will save lots of bandwidth as each computer will not

download updates individually. WSUS 3.0 SP1 is the only version of WSUS that can be installed on Windows Server 2008. Earlier versions of WSUS cannot be installed on a server running Windows Server 2008.

Answer: C is incorrect. Read-only Domain Controller (RODC) is a domain controller that hosts the read-only partition of the Active Directory database. RODC was developed by Microsoft typically to be deployed in a branch office environment.

RODC is a good option to enhance security by placing it in a location where physical security is poor. RODC can also be placed at locations having relatively few users and a poor network bandwidth to the main site. As only the read-only

partition of the Active Directory database is hosted by RODC, a little local IT knowledge is required to maintain it.

Answer: A is incorrect. DNS dynamic update is used to enable DNS client computers for registering and dynamically updating their resource records with a DNS server whenever any modification or change has been taken place. It is used to

update the DNS client computers with the reflecting changes.

---

**QUESTION 6**

Kerberos prevents:

A. Denial of Service attacks

B. spyware distribution

C. file corruption

D. replay attacks

Correct Answer: D

---

**QUESTION 7**

Which two are included in an enterprise antivirus program? (Choose two.)

A. Attack surface scanning

B. On-demand scanning

C. Packet scanning

D. Scheduled scanning

Correct Answer: BD

---

**QUESTION 8**

You have an application that communicates by using plain text. You want to secure communications between the application and a server at the network layer. What should you implement?

A. TLS

B. SFTP

C. SSH

D. IPsec

Correct Answer: D

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an Internet Protocol network. It operates at the network (layer 3 in the OSI model)

Incorrect Answers:

A, C: TLS and SSH are cryptographic protocols designed to provide communications security over a network. They operate at the application layer, or layer 7 of the OSI model.

B: SFTP provides file access, file transfer, and file management over a reliable data stream. It operates at the application layer, or layer 7 of the OSI model.

References: https://en.wikipedia.org/wiki/IPsec https://en.wikipedia.org/wiki/Transport_Layer_Security https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol

---

**QUESTION 9**

Which of the following is a secret numeric password shared between a user and a system for authenticating the user to the system?

A. PIN

B. Private key

C. Key escrow

D. Public key

Correct Answer: A

A personal identification number (PIN) is a secret numeric password shared between a user and a system for authenticating the user to the system. Answer: C is incorrect. Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees\\' private communications, or governments, who may wish to be able to view the contents of encrypted communications. Answer: B is incorrect. In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. Answer: D is incorrect. A Public Key is known commonly to everybody. It is used to encrypt data. Only specific users can decrypt it. Data encryption is used to encrypt data so that it can only be decrypted with the corresponding private key owned by the public key owner. The public key is also used to verify digital signatures. This signature is created by the associated private key.

---

**QUESTION 10**

Which of the following practices should be followed to keep passwords secure? Each correct answer represents a complete solution. Choose three.

A. Change the passwords whenever there is suspicion that they may have been compromised.

B. A password should be alpha-numeric.

C. A password should not be more than five words.

D. Never write down a password.

Correct Answer: ABD

Answer: D, A, and B

The following practices should be followed to keep passwords secure: Never write down a password.

Change the passwords whenever there is suspicion that they may have been compromised. A password should be alpha-numeric. Never use the same password for more than one account. Never tell a password to anyone, including people

who claim to be from customer service or security.

Never communicate a password by telephone, e-mail, or instant messaging. Ensure that an operating system password and application passwords are different. Make passwords completely random but easy for you to remember.

---

**QUESTION 11**

Mark works as a Network Administrator for TechMart Inc. The company has a Windows-based network. Mark wants to implement stronger authentication measures for the customers, as well as eliminate IT staff from logging on with high privileges. Mark has various options, but he is required to keep the processes easy for the helpdesk staff. Which of the following is a service can the staff uses as an alternative of signing in with elevate privileges?

A. Secondary Logon-Run As

B. Security log

C. Hardware firewall

D. Encrypted network configuration

Correct Answer: A

Secondary Logon (Run As) is defined as a starting programs and tools in local administrative context. Windows secondary logon is used to permit administrators to log on with a non-administrative account and be able to perform the several administrative tasks without logging off by using trusted administrative programs in administrative contexts. Answer: B is incorrect. The security log is generated by a firewall or other security device. It is used to define list of events that could affect the security of data or infrastructure, such as access attempts or commands, and the names of the users participating in this illegal process. Answer: C is incorrect. Hardware firewall is defined as the important part of the system and network set-up on a broadband connection. It can be effective with small or no configuration, and is used to protect every machine on a local network. The hardware firewalls will have at least four network ports for connecting to other computers. This type of firewall uses packet filtering for checking the header of a packet in order to check its source and destination. The information obtained in this manner is compared to a set of predefined or user-created rules and then the packet is forwarded or dropped.

---

**QUESTION 12**

You need to prevent unauthorized users from reading a specific file on a portable computer if the portable computer is stolen.

What should you implement?

A. File-level permissions

B. Advanced Encryption Standard (AES)

C. Folder-level permissions

D. Distributed File System (DFS)

E. BitLocker

Correct Answer: E

Reference: http://4sysops.com/archives/seven-reasons-why-you-need-bitlocker-hard-drive-encryption-for-your-whole-organization/